



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,403	07/26/2001	William Michael Raike	P65847US1	4247

7590 12/16/2004

JACOBSON HOLMAN
PROFESIONAL LIMITED LIABILITY COMPANY
400 SEVENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/912,403	Applicant(s) RAIKE, WILLIAM MICHAEL	
	Examiner Minh Dieu Nguyen	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-8 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) and further in view of Levy et al (6,212,633).

a) As to claims 1 and 6, Wasilewski discloses methods for providing conditional access information to decoders in a packet-based multiplexed communications system comprising a transmitter (Fig. 2, element 198) encrypts payload sections of each transport packet stream of data (col. 9, lines 30-36) that assigned a unique packet ID (PID) (col. 8, lines 44-46) using unique encryption control words (col. 9, lines 26-30); transmitter adds the packet ID to the corresponding encrypted packet data; inserts the packet so processed into the packet stream and transmit the encrypted data packet stream to the recipient (Figs. 3A and 3B). Wasilewski also discloses at the recipient's station (Fig. 2, element 201), each received encrypted packet is decrypted by the decryption information respective to each packet ID (Fig. 6; col. 14, lines 13-20) and

the decrypted packet data is outputted in a form suitable for playing the streamed media (Fig. 2, element 208).

Wasilewski does not disclose the encryption key used for encrypting packet data is created by computing a secure hash of a base key and the assigned tag value of the packet.

Bleichenbacher discloses a system for transmitting an encrypted program together with a program identifier which is used by a set top terminal, together with stored entitlement information, to derive the decryption key necessary to decrypt the program (col. 1, lines 9-15), the system comprising a program key used to encrypt each program (col. 3, lines 4-6), the program key is created by applying a hash function to the master key and program identifier (col. 3, lines 30-37). The master key which reads on the base key may be updated for security reason (col. 7, lines 21-23). Bleichenbacher also discloses the decryption process (Fig. 9).

Both Wasilewski and Bleichenbacher do not disclose encrypting the base key to create an open key and transmit the open key to the recipient.

Levy discloses a secure data communication incorporating data encryption and/or access control comprising the steps of generating randomly a session key, encrypting the session key (col. 13, line 64 to col. 14, line 3) and transmit the encrypted session key to target node (col. 14, lines 15-17).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing hash function of base key and packet ID as Bleichenbacher teaches in the system of Wasilewski and the use of encrypting the base

key as Levy teaches in the system of Wasilewski and Bleichenbacher so as to enhance the security of transmitted information.

b) As to claims 2 and 7, Wasilewski discloses the encryption control word is transmitted to the recipient by adding it to the stream header (Fig. 3B) and then extracted from the stream header at the recipient's station for decryption (Fig. 6).

Wasilewski does not disclose the open key is transmitted.

Levy discloses the encrypted session key is transmitted to the target node (col. 14, lines 15-17).

c) As to claim 3, Levy discloses the base key is encrypted using a public key encryption algorithm in conjunction with the recipient's public key and wherein the open key is decrypted using the public key encryption algorithm in conjunction with the recipient's private key (col. 13, line 64 to col. 14, line 3).

d) As to claim 4, Wasilewski discloses the packet data is encrypted using a symmetric encryption algorithm in conjunction with the packet key and the encrypted data is decrypted at the recipient's station using the symmetric encryption algorithm in conjunction with the recreated packet key (col. 3, line 45 to col. 4, line 6).

e) As to claims 5 and 8, Bleichenbacher discloses the hash function used to create and reestablish the packet key is SHA-1 or MD5 (col. 5, lines 43-47).

Conclusion

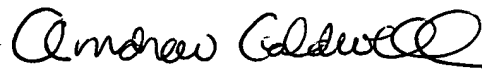
4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.


mdn
12/8/04

Minh Dieu Nguyen
Examiner
Art Unit 2137


Andrew Caldwell